COMP:0278
P01-4017

METHOD FOR IDENTIFYING THE WRITE PROTECT STATUS OF A DISKETTE

BY:

CHRISTOPHER J. FRANTZ
E. DAVID NEUFELD

"EXPRESS MAIL" MAILING LABEL
Number: ***EV 017 056 882 US***
Date of Deposit: ***January 10, 2002***

Pursuant to 37 C.F.R. § 1.10, I hereby certify that I am personally depositing this paper or fee with the U.S. Postal Service, "Express Mail Post Office to Addressee" service on the date indicated above in a sealed envelope (a) having the above-numbered Express Mail label and sufficient postage affixed, and (b) addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature: Carla DeBlaw
Printed Name: *Carla Deblaw*

METHOD FOR IDENTIFYING THE WRITE PROTECT STATUS OF A DISKETTE

BACKGROUND OF THE INVENTION

1. Field Of The Invention

The present technique relates generally to removable storage media, such as computer diskettes, which comprise a write protect mechanism. More particularly, the present technique provides a method for identifying the write protect status of the removable storage media prior to accessing the media and automatically upon inserting the media into a media drive.

2. Background Of The Related Art

This section is intended to introduce the reader to various aspects of art which may be related to various aspects of the present invention which are described and/or claimed below. This discussion is believed to be helpful in providing the reader with background information to facilitate a better understanding of the various aspects of the present invention. Accordingly, it should be understood that these statements are to be read in this light, and not as admissions of prior art.

Removable storage media, such as computer diskettes, often have write protect mechanisms to control data storage to the media. For example, 3-1/2 inch floppy diskettes have a write protect mechanism comprising an aperture and a slider that is movable over the aperture. If the slider covers the aperture, such that the aperture is closed, then data can be written to the

floppy diskette. However, if the slider is moved away from the aperture, then the floppy diskette is write protected. In certain applications, it is desirable to know the write protect status of the removable storage media prior to accessing the media or attempting storage to the media. Unfortunately, the write protect status of the removable storage media is typically determined by physically observing the write protect mechanism or by attempting to store data to the media during normal storage operations.

Accordingly, a technique is needed for identifying the write protect status of the removable storage media, such as a computer diskettes, prior to accessing the media or attempting storage to the media. It also would be advantageous to identify the write protect status of the removable storage media automatically upon insertion into a media drive.

BRIEF DESCRIPTION OF THE DRAWINGS

Certain advantages of the invention may become apparent upon reading the following detailed description and upon reference to the drawings in which:

Fig. 1 is a block diagram illustrating an exemplary system of the present technique; and

Figs. 2 and 3 are flow charts illustrating exemplary processes for identifying the write protect status of a media.

DESCRIPTION OF SPECIFIC EMBODIMENTS

One or more specific embodiments of the present invention will be described below. In an effort to provide a concise description of these embodiments, not all features of an actual implementation are described in the specification. It should be appreciated that in the development of any such actual implementation, as in any engineering or design project, numerous implementation-specific decisions must be made to achieve the developers' specific goals, such as compliance with system-related and business-related constraints, which may vary from one implementation to another. Moreover, it should be appreciated that such a development effort might be complex and time consuming, but would nevertheless be a routine undertaking of design, fabrication, and manufacture for those of ordinary skill having the benefit of this disclosure.

Turning now to the drawings and referring initially to Fig. 1, a block diagram of an exemplary system in which the present invention may be practiced is illustrated and designated using a reference numeral 10. As illustrated, the system comprises a computing device 12 communicatively coupled to a plurality of remote devices via a network 14. For example, the computing device 12 may communicate through the network 14 with personal computers 16 and 18, a server 20 (e.g., a headless server), a workstation 22, and a computing device 24. The computing devices 12 and 24 may embody any desired stationary or mobile computing device, such as a desktop computer, a laptop computer, a personal digital assistant, a workstation, a server, or any other processor-based device. Accordingly, the computing devices 12 and 24 may comprise a variety of software and hardware, such as an operating system, application programs,

circuitry, a processor, random access memory, read only memory, a hard disk drive, CD/DVD drives, a floppy disk drive, audio/video devices (e.g., a monitor), input/output devices (e.g., a keyboard, a mouse, etc.), and various other components.

In this exemplary embodiment, the computing device 12 comprises a media drive 26 for a removable media 28, which may embody a variety of storage media such as a computer diskette (e.g., a floppy diskette). The removable media 28 also has a write protect mechanism 30 for protecting data on the media 28. For example, the write protect mechanism 30 may comprise a slider mechanism that is movable between open and closed positions over an aperture. As described in detail below, the present technique identifies the write protect status of the write protect mechanism 30 prior to accessing the media or attempting storage to the media during normal operations.

The write protect status of the write protect mechanism 30 may be desired by the computing device 12 or any of the remote devices 16 through 24. For example, the headless server 20 may desire interaction with the removable media 28 for software/hardware configuration of the server 20. Moreover, any of the remote devices 16 through 24 may interact with the removable media 28 to access data, to access program files, to access a desired operating system, or to perform any desired operation disposed on the media 28. For example, one computer may interact with another computer to perform remote management functions, which may require interaction with the removable media 28. Accordingly, the following write protect identification techniques are intended for both local and network computer systems.

Figs. 2 and 3 are flow charts illustrating exemplary processes 100 and 200 for identifying the write protect status of the removable media 28. Processes 100 and 200 may be performed at any time by the host computer system or a remote computer system, such as discussed above with reference to Fig. 1. For example, the host or remote computer systems may initiate processes 100 or 200 upon insertion of the removable media 28 into the media drive 26, upon an access request by the host or remote computer system, or at any other suitable time.

As illustrated in Fig. 2, the process 100 proceeds to identify the write protect status by identifying the media type of the removable media 28 (block 102), seeking to a location beyond the storage area of the removable media 28 (block 104), and then attempting to write data to the removable media 28 at the location (block 106). For example, the process 100 may identify the removable media 28 as a floppy diskette (e.g., a 3-1/2 inch computer diskette) and seek past the end of storage tracks and sectors to a non-storage location in which data cannot be stored on the removable media 28. Accordingly, the attempt by process 100 to write data to the removable media 28 at the non-storage location fails, as expected (block 108). The process 100 then identifies the write protect status of the removable media 28 by evaluating the failure code generated by the attempted write to the non-storage location (block 110). For example, the process 100 may cause a failure code, such as ERROR_WRITE_PROTECT, which indicates that data cannot be written to the removable media 28 (block 112). If the attempted write at block 106 produces the foregoing failure code at block 112, then the process 100 identifies the write protect status of the removable media 28 as write protected (block 114). However, the process

100 also may fail by another failure code, such as ERROR_ INVALID_PARAMETER, which may indicate that data cannot be written to the removable media 28 at the non-storage location (block 116). If the attempted write at block 106 produces the foregoing failure code at block 116, then the process 100 identifies the write protect status of the removable media 28 as not write protected (block 118). However, in either case, data is not written to the removable media 28.

As illustrated in Fig. 3, the present technique may interact with the removable media 28 in any suitable manner that produces one or more error codes, which may be used to identify the write protect status of the media 28. Process 200 proceeds to identify the write protect status by reading data from the removable media 28 at a storage location (block 202), attempting to write the data back to the removable media 28 at the same storage location (block 204), and then querying whether the attempted write has failed (block 206). If the attempted write fails, then the process 200 observes a write failure code, such as ERROR_WRITE_PROTECT (block 208). The process 200 then evaluates the write failure code observed at block 208 and identifies the write protect status of the removable media 28 as write protected (block 210). However, if the attempted write does not fail, then the process 200 proceeds to write the data over the existing data at the storage location (block 212). Accordingly, the process 200 evaluates the successful write at block 212 and identifies the write protect status of the removable media 28 as not write protected (block 214).

While the invention may be susceptible to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and will be described in detail herein. However, it should be understood that the invention is not intended to be limited to the particular forms disclosed. Rather, the invention is to cover all modifications, equivalents and alternatives falling within the spirit and scope of the invention as defined by the following appended claims. For example, the systems and methods described above may be performed locally or remotely by any suitable computer hardware and software, which may produce a variety of failure codes that may be utilized by the present technique to identify the write protect status of the removable media. Moreover, the present technique may provide custom failure codes associated with a write protect identification program, which may be disposed on a host or remote computer system.